BUSINESS CONTINUITY PLAN

Pursuant to Regulation 121, IFSCA (Fund Management) Regulations, 2025

DOCUMENT CONTROL

Field	Details
Title	Business Continuity Plan
Policy Owner	Compliance Department
Preparer and Reviewer	Compliance Officer
Approved by	Directors
Version	V1
Regulatory Reference	Regulation 121, IFSCA (Fund Management) Regulations, 2025 (as amended up to July 30, 2025); IFSCA Cyber Security and Cyber Resilience Guidelines, March 10, 2025 (as amended March 10, 2026)
Effective Date	April 30, 2026
Next Review	On any Regulatory change or Annual, whichever is earlier

VERSION SUMMARY

Version	Policy Reviewed	Review Date	Department	Approved by
V1	Business Continuity Plan	30.04.2026	Compliance	Directors

Table of Contents

1. Title / Objective 3
2. Regulatory Background 3
3. Applicability 3
4. Implementation / Process 4
   4.1 Critical Business Functions and Recovery Objectives 4
   4.2 List of Important Documents and Records 4
   4.3 Risk Scenarios and Responses 5
   4.4 Data Backup and Recovery 6
   4.5 Client Communication and Vendor Co-ordination 7
   4.6 Annual BCP Testing and Review 7
5. Policy Review 7
6. Responsibility 7
7. Power to Remove Difficulties 7
8. Effective Date 8

1. Title / Objective

The objective of this Business Continuity Plan ("BCP") is to ensure that T-Cap Financial Services IFSC Private Limited ("T-Cap" or "the FME"), as a registered Fund Management Entity, has comprehensive procedures in place to address emergencies or significant business disruptions. It aims to maintain operational resilience and minimise the impact of disruptions on the FME's operations, protect client interests, maintain compliance with all regulatory requirements, and minimise operational downtime.

2. Regulatory Background

This Business Continuity Plan is established pursuant to the following regulatory requirements:

- Regulation 121 of the IFSCA (Fund Management) Regulations, 2025 (F. No. IFSCA/GN/2025/002, in force from February 13, 2025, as amended up to July 30, 2025) ("FM Regulations, 2025"), which mandates every registered FME to establish and maintain a plan to address emergencies and disruptions, ensuring the FME's ability to continue essential operations.
- IFSCA Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs, issued vide Circular No. IFSCA-CSD0MSC/13/2025-DCS dated March 10, 2025, effective April 1, 2025 ("Cyber Security Guidelines"), which mandate regulated entities to implement Business Continuity and Disaster Recovery arrangements as part of their Cyber Security and Cyber Resilience Framework.
- Amendment to the Cyber Security Guidelines issued vide Circular No. IFSCA-CSD0MSC/1/2026-DCS dated March 10, 2026, which clarifies exemption conditions and annual certification requirements applicable to certain categories of regulated entities, including those operating as branches or entities with fewer than 10 employees.

This BCP is designed to align T-Cap's operational resilience practices with all applicable regulatory requirements. Any subsequent amendment or circular issued by the IFSCA shall automatically apply, and this BCP shall be read and updated accordingly.

3. Applicability

This Business Continuity Plan applies to all operations of T-Cap as a registered FME under the FM Regulations, 2025. It covers procedures and protocols for handling emergencies or significant business disruptions, encompassing various scenarios that may impact operations, including natural disasters, technology failures, cybersecurity incidents, key personnel unavailability, or other unforeseen events.

4. Implementation / Process

This plan establishes procedures and processes to maintain operational continuity based on three primary categories of disruptions, which may occur individually or in any combination:

- Loss of access to parts of, or the entire, facility (e.g., following a fire, storm, flooding, or government-imposed lockdown);
- Loss of services due to a reduction in workforce (e.g., pandemic, illness, or unavailability of key personnel); and
- Loss of services due to equipment or systems failure (e.g., IT systems failure, electrical grid failure, or cybersecurity incident).

4.1 Critical Business Functions and Recovery Objectives

The following critical business functions have been identified, along with their Recovery Time Objectives (RTO) and designated alternate processes:

Critical Business Function	Recovery Time Objective (RTO)	Alternate Process
Investment Decision-Making	1 Business Day	Temporarily halted until system access restored; pre-authorised standby instructions to be activated
Trade Execution	1 Business Day	Manual execution via broker assistance; direct telephonic instructions to custodian/broker
NAV Calculation / Reporting	2 Business Days	Coordination with fund administrator; manual calculation based on last known data
Client Communications & Vendor Co-ordination	Same Day	Alternate email, mobile channels, and secure video conferencing tools
Regulatory Filings	Within prescribed timeline	Extensions requested from IFSCA if necessary; advance notice to be provided
Cybersecurity Incident Response	Immediate (within 6 hours of detection)	Activate Cyber Incident Response Protocol; notify IFSCA at cyber-incidents@ifsca.gov.in; engage parent entity IT team (Trust Investment Advisors Pvt. Ltd.)

4.2 List of Important Documents and Records

T-Cap shall maintain the following records and documents in accordance with the FM Regulations, 2025 and applicable IFSCA circulars. All records shall be maintained for a period of at least eight (8) years in electronic form, consistent with the records retention standards applied across IFSCA regulated entities:

- A copy of the profit and loss account for each accounting period;
- A copy of the auditor's report on the accounts for each accounting period;
- A statement of net worth for each quarter;
- Documents relating to compliance with AML/CFT guidelines;
- Documents relating to account opening of each client, and any power of attorney or signature authority forms of clients;
- Relevant records and documents relating to activities under the FM Regulations, 2025;
- Such other books of accounts, records, and documents as may be specified by the IFSCA from time to time;
- Records describing the assets under each scheme, valuation policies and practices, investment strategies, particulars of investors and their contributions, and the rationale for investments made; and
- Cyber security audit reports and annual certifications as required under the IFSCA Cyber Security Guidelines.

4.3 Risk Scenarios and Responses

T-Cap has established the following protocols to address identified risk scenarios:

a. Technology or System Failure

In the event of a technology or system failure, including a malfunction in the portfolio management system or connectivity issues affecting access to investment platforms, the team will activate the following measures: secure, cloud-based platforms with automatic daily backups and system redundancy are maintained to mitigate such risks; employees will access systems via secure connections from remote locations; and essential functions such as trade execution and client reporting will be continued through manual processes or direct coordination with service providers and brokers until full system restoration is achieved.

b. Office Inaccessibility

Whenever primary office premises become inaccessible due to a natural disaster, public emergency, or government-imposed lockdown, the team will transition to a remote working environment. All employees are equipped with necessary hardware and secure internet access to perform their duties remotely. Communication will be maintained through encrypted email, video conferencing, and dedicated mobile channels. Since core applications and files are cloud-hosted, access to critical data remains uninterrupted.

c. Key Personnel Unavailability

In the event of the unavailability of key personnel due to illness, accident, or other emergencies, roles and responsibilities are clearly documented and accessible to all team members. This enables another employee or an authorised external consultant to temporarily assume the required functions. If the Principal Officer is unavailable, the Compliance Officer or a pre-designated senior advisor may step in to ensure continuity of critical operations and regulatory responsibilities. T-Cap shall promptly inform the IFSCA of any such material change in KMP status as required under the FM Regulations, 2025.

d. Cybersecurity Incident

All cybersecurity functions are centrally managed by the parent entity, Trust Investment Advisors Private Limited, Mumbai. In the event of a cyber-breach or data compromise, the following protocol shall be activated:

- Immediate isolation of affected systems and containment of the breach;
- Restoration of data from secure, geographically redundant backups;
- Notification to IFSCA within six (6) hours of detection of the incident at cyber-incidents@ifsca.gov.in with a copy to the designated CISO;
- Submission of an interim report to IFSCA within three (3) days of detection;
- Submission of a detailed root cause analysis report to IFSCA within thirty (30) days of detection; and
- Investigation, remediation, and full system restoration under the oversight of the parent entity's IT team.

Since T-Cap operates as an entity whose cybersecurity functions are managed by its regulated parent entity (Trust Investment Advisors Private Limited), it may be eligible for the three-year exemption from direct compliance with certain provisions of the Cyber Security Guidelines, as amended by the IFSCA Circular dated March 10, 2026, subject to fulfilment of the following conditions:

- Adoption of the Cyber Security and Cyber Resilience Framework and Information Security Policy of the parent entity;
- The CISO of the parent entity to act as the Designated Officer for T-Cap;
- The parent entity to be regulated by a regulator or Government Body in its home jurisdiction;
- The Designated Officer to certify annually that all necessary systems and processes are in place, and to submit such certification to the IFSCA within ninety (90) days of the end of each financial year; and
- Submission of the annual cyber security audit report to IFSCA.

4.4 Data Backup and Recovery

T-Cap relies on secure, cloud-based systems, including Microsoft OneDrive, for data storage and accessibility. All critical business and client data — including client records, fund documentation, investment reports, and compliance files — are backed up periodically, with secure version history maintained to enable quick restoration if needed. These backups are encrypted and stored in geographically redundant locations to ensure data integrity and availability in the event of a system failure or cyber incident. Regular monitoring and periodic testing are conducted to verify the effectiveness of the backup and recovery process.

Backup systems shall be tested at least annually, and test results shall be documented and made available for regulatory inspection.

4.5 Client Communication and Vendor Co-ordination

In the event of any significant disruption affecting client assets or reporting, T-Cap shall ensure timely communication with clients primarily through email and mobile contact, and secondarily via website updates or SMS alerts. Clients will be informed within twenty-four (24) hours of any material impact on their portfolios or reporting.

Key third-party service providers, including the fund administrator, custodian, auditor, and legal counsel, are integrated into this Business Continuity Plan. Regular co-ordination is maintained with these vendors to ensure alignment of contingency measures and seamless operational support during disruptions. Third-party vendor cybersecurity risks shall be assessed periodically, and vendors shall be required to meet the data security and incident reporting standards mandated under the IFSCA Cyber Security Guidelines.

4.6 Annual BCP Testing and Review

T-Cap shall conduct at least one BCP drill or table top exercise annually to test the adequacy of its business continuity and disaster recovery procedures. The results of such exercises shall be documented and used to update and improve this Plan. The BCP testing shall cover, at a minimum, the critical business functions identified in Section 4.1 and the cybersecurity incident response protocol described in Section 4.3(d).

5. Policy Review

T-Cap will conduct a comprehensive annual review of this Business Continuity Plan to assess its adequacy and effectiveness in addressing emergencies and significant business disruptions. Additionally, this Plan shall be reviewed and updated promptly upon any amendment to the FM Regulations, 2025, any IFSCA circular relating to business continuity or cybersecurity, or any material change in T-Cap’s operations or risk profile.

6. Responsibility

The Directors hold overall responsibility for the approval and oversight of this Business Continuity Plan. The Compliance Officer designated under Regulation 7(2) of the FM Regulations, 2025 is responsible for the day-to-day implementation, monitoring, and periodic review of this Plan. The Compliance Officer shall also be responsible for co-ordinating with the parent entity’s Designated Officer (CISO) for cybersecurity-related continuity matters, and for submitting annual certifications and audit reports to the IFSCA as required under the Cyber Security Guidelines.

7. Power to Remove Difficulties

In the event of any difficulties or ambiguities arising during the implementation of this Plan, the Directors are empowered to provide necessary clarifications or make amendments as deemed necessary, ensuring the smooth and effective enforcement of this BCP. Any such clarifications

or amendments shall be documented and, where material, shall be communicated to all relevant personnel.

8. Effective Date

This Business Continuity Plan (Version V1) is effective from April 30, 2026 upon approval by the Directors of the Company. All operations of T-Cap must comply with the provisions of this Plan from the above effective date.

***